UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/091,645	03/05/2002	Handong Wu	NETAP019	9146

28875 7590 08/18/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/091,645	WU ET AL.	
	Examiner	Art Unit	
	Farid Homayounmehr	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 March 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 March 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *04/29/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-20 have been examined.

Information Disclosure Statement PTO-1449

The Information Disclosure Statement submitted by applicant on 09/14/2000 has been considered. Please see attached PTO-1449.

Claim Objections

1. Claim 20 is objected to because of the following informalities: typo error Examiner suggests changing 'computer readable medium' to 'computer-readable storage medium'.

Claim Rejections - 35 USC § 101

2. Claims 19 and 20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Data signal embodied in a carrier wave is not statutory.

2.1. As per claim 19, computer program product comprised of a computer-readable storage medium. As described in page 14 of the specifications, one type of computer-readable storage medium is 'a data signal embodied in a carrier wave'.

2.2. As per claim 20, computer-readable storage media is selected from a group consisting data signal embodied in a carrier wave.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1 to 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Vaidya (US Patent No. 6,279.113).

3.1. As per claims 1, Vaidya is directed to an intrusion detection and analysis system (Fig.1 column 5 lines 5 to 9) comprising:

a data monitoring device comprising a capture engine operable to capture data passing through the network (Fig. 1, item 10 column 5, lines 9 to 25) and configured to monitor network traffic (Fig. 1, item 10 column 5, lines 13 to 15, see also Fig. 4 item 36 column 7 lines 11 to 15), decode protocols (Fig. 2, item 36 within item 10, column 7 lines 17 to 24), and analyze received data (column 6 line 57 to column 7 line10);

an intrusion detection device (Fig 2, item 36) comprising a detection engine operable to perform intrusion detection on data provided by the data monitoring device (item 36 column 6 lines 7 to 13);

application program interfaces configured to allow the intrusion detection device access to applications of the data monitoring device to perform intrusion detection. Application program interface is defined as 'a set of functions or methods used to access some functionality'. Referring to Fig. 2, the configuration builder module (item 32) allows the intrusion detection

device (item 36) access attack signature profiles stored in signature profile memory (item 39), as described in column 6 lines 1 to 11. Also, the communication module (item 34) allows intrusion detection device access the data in database handler (item 26). This clearly allows the intrusion detection device access the functionality of the data-monitoring device to perform intrusion detection, and hence discloses the feature. Therefore, the Examiner asserts that Vaidya discloses the feature by inheritance.

memory for storing reference network information used by the intrusion detection device to determine if an intrusion has occurred (Fig 2, item 26, column 5 lines 46 to 50).

3.2. As per claim 2, Vaidya continues to teach a reference network information comprises a signature database including signature profiles associated with a known network security violation (Fig 2, item 39 column 6 lines 1 to 7) and wherein the detection engine (item 32) is operable to compare the data provided by the data monitoring device (item 39) with the signature profiles to detect network intrusions (column 6 lines 7 to 18).

3.3. As per claim 3, Vaidya is directed to a parser (Fig. 4 item 36) operable to parse (referring to Fig. 8 and column 9 lines 45 to 55, and Fig. 9 and column 10 line 17 to column 11 line 15, the data collector, as part of processing the attack signature profile, separates the fields in the signature profile, which is equivalent to parsing), generate (Fig. 2 and 3 and column 6 lines 27 to 29), and load (Fig. 2 column 6 lines 1 to 11 and Fig. 4 column 7 lines 18 to 23) signatures at the detection engine.

3.4. As per claim 4, Vaidya is directed to the reference network information comprises a baseline state of network traffic (state cache as shown in Fig. 4 item 44 and described in column 9 lines 3 to 20 stores the network traffic state data) and wherein the detect engine is operable to compare the data received by the capture engine to the baseline network state and look for anomalies (claims 11 and 12).

3.5. As per claim 5, Vaidya is directed to a data-monitoring device in accordance with claim 4 that provides the baseline state of network traffic. Vaidya provides the baseline state of network traffic in the virtual processor (Fig. 4 item 36), wherein the Register Cache stores the information extracted from a packet (as described in column 7 lines 11 to 17), and in the case where a sequential or timer/counter based signature profiles are invoked (column 7 lines 48 to 51), the state of network traffic (data extracted from the packet) is saved in the state cache (Fig 4. item 44) and used in conjunction with the data from the subsequent packet (column 7 lines 59 to 65) to determine network anomalies. The use of traffic state data to detect network anomalies is further described in

column 8 lines 16 to 40.

3.6. As per claim 6, Vaidya is directed to a log file configured to at least temporarily store reports generated by the detect engine, on account of the Reaction Module (Fig. 2 item 38), which receives alerts from the detection device whenever a network intrusions is detected, and initiates reactions depending on nature of the attack (column 6 lines 18 to 26).

3.7. As per claim 7, Vaidya is directed to a system according to claim 6, further comprising an alarm manager operable to generate alarms based on the information in the log file (column 6 lines 21 to 26).

3.8. As per claim 8, Vaidya discloses a system in accordance with claim 1 further comprising a filter configured to filter out packets received at the data-monitoring device. Filter is defined as 'a device that separates data in accordance with specific criteria'. Item 96 in Fig. 6 (which describes the operation of the data collector) returns 'No Entry Found' when the data collected from the packet indicates that the packet's destination server is not being monitored, and no further action will take place on that packet (column 8 lines 58 to 65). This clearly discloses 'a separation of packets based on a criteria' and hence discloses a 'filter'. Vaidya does not specifically refer to a filter. Therefore, the Examiner asserts that it Vaidya discloses the feature.

3.9. As per claim 9, Vaidya discloses a system in accordance with claim 1 further comprising a statistics collector operable to collect statistics on packets received by the data-monitoring device. Statistics is defined as 'the analysis of population characteristics by inference from sampling'. The data collector performs intrusion detection by measuring the number of times a file or an object is accessed during a specific time period (column 8 lines 15 to 40 and column 9 lines 4 to 21). This clearly works based on the number (population) of packets accessing a file or an object, and hence discloses a collection of statistics. Vaidya does not specifically refer to a statistics collector. Therefore, the Examiner asserts that Vaidya discloses the feature.

3.10. As per claim 10, Vaidya is directed to a system in accordance with claim 1 wherein the capture engine is configured to forward packets and temporarily store packets for later analysis by data monitoring device (Fig. 4 item 40 column 7 lines 15 to 24).

3.11. As per claim 11, Vaidya is directed to a method for performing intrusion detection with an intrusion detection and analysis system (Fig.1 and column 5, as described in lines 5 to 9) comprising a data monitoring device configured to monitor network traffic (Fig. 1, item 10 column 5, lines 13 to 15, see also Fig. 4 item 36 column 7 lines 11 to 15), decode

protocols (Fig. 2, item 36 within item 10, column 7 lines 17 to 24), and analyze received data (column 6 line 57 to column 7 line10) and an intrusion detection device (Fig 2, item 36) coupled to data monitoring device (Fig. 2 items 34 and 30 couple the intrusion detection device to the data collected by the data monitoring device) and configured to perform intrusion detection on data provided by the data monitoring device (column 6 lines 1 to 21); the method comprising:

receiving data at data monitoring device (Fig 4. item 36 column 7 lines 18 to 24);

capturing at least a portion of the packets contained within the data (column 7 lines 18 to 24);

calling an application program interface configured to open application of the data monitoring device; and performing intrusion detection at the intrusion detection device utilizing at least one of the applications of the data monitoring device. Application program interface is defined as 'a set of functions or methods used to access some functionality'. Referring to Fig. 2, the configuration builder module (item 32) allows the intrusion detection device (item 36) access attack signature profiles stored in signature profile memory (item 39), as described in column 6 lines 1 to 11. Also, the communication module (item 34) allows intrusion detection device access the data in database handler (item 26). This clearly allows the intrusion detection device access the functionality of the data-monitoring device to perform intrusion detection, and hence discloses the feature. Vaidya does not specifically refer to an application program interface to access the data and functionalities of the data-monitoring device. Therefore, the Examiner asserts that Vaidya discloses the feature.

3.12. As per claim 12, Vaidya discloses a method of claim 11 wherein calling an application program interface comprises calling an application program interface configured to open a protocol decoding application. As described in section 1.11, Vaidya discloses the features of an application program interface. In addition, Vaidya discloses the feature of a protocol decoding application (Fig. 2, item 36 within item 10, column 7 lines 17 to 24). Therefore, the Examiner asserts that Vaidya does disclose the entire feature.

3.13. As per claim 13, Vaidya discloses a method of claim 11 wherein calling an application program interface comprises calling an application program interface configured to open an alarm generation application. As described in section 3.11, Vaidya discloses the features of an application program interface. In addition, Vaidya discloses the feature of an alarm generation application (column 6 lines 21 to 26). Therefore, the Examiner

asserts that Vaidya does disclose the entire feature.

3.14. As per claim 14, Vaidya discloses a method of claim 11 further comprising filtering prior to capturing packets. Filtering is defined as 'a method to separate data in accordance with specific criteria'. Item 96 in Fig. 6 (which describes the operation of the data collector) returns 'No Entry Found' when the data collected from the packet indicates that the packet's destination server is not being monitored, and no further action will take place on that packet (column 8 lines 58 to 65). This clearly discloses 'a separation of packets based on a criteria' and hence discloses 'filtering'. Vaidya does not specifically refer to filtering. Therefore, the Examiner asserts that Vaidya discloses the feature.

3.15. As per claim 15, Vaidya discloses a method of claim 11 wherein performing intrusion detection comprises performing signature matching (Fig. 4 column 7 line 31 to column 8 line 40 and claim 1).

3.16. As per claim 16, Vaidya discloses a method of claim 15 wherein the application program interfaces provide parsing of signatures used in signature matching (column 10 lines 17 to 45).

3.17. As per claim 17, Vaidya discloses a method of claim 11 further comprising analyzing the data at the data-monitoring device (column 6 line 57 to column 7 line10).

3.18. As per claim 18, Vaidya discloses a method of claim 11 wherein performing intrusion detection comprises detecting anomalies in the received data (column 6 line 57 to column 7 line10).

3.19. As per claim 19, Vaidya discloses a computer program product (in form of a set of instructions to be sequentially executed as described in column 16 claim 18) for performing intrusion detection with an intrusion detection and analysis system comprising a data monitoring device configured to monitor network traffic (Fig. 1 column 5 lines 5 to 9) comprising a data monitoring device configured to monitor network traffic (Fig. 1, item 10 column 5, lines 13 to 15, see also Fig. 4 item 36 column 7 lines 11 to 15), decode protocols (Fig. 2, item 36 within item 10, column 7 lines 17 to 24), and analyze received data (column 6 line 57 to column 7 line10) and an intrusion detection device (Fig 2, item 36) coupled to data monitoring device (Fig. 2 items 34 and 30 couple the intrusion detection device to the data collected by the data monitoring device) and configured to perform intrusion detection on data provided by the data monitoring device (column 6 lines 1 to 21); the product comprising:

code that receives data at data monitoring device (Fig 4. item 36 column 7 lines 18 to 24);

code that captures at least a portion of the packets contained within the data (column 7 lines 18 to 24);

code that calls an application program interface configured to open application of the data monitoring device; and performs intrusion detection at the intrusion detection device utilizing at least one of the applications of the data monitoring device. (Application program interface is defined as 'a set of functions or methods used to access some functionality'. Referring to Fig. 2, the configuration builder module (item 32) allows the intrusion detection device (item 36) access attack signature profiles stored in signature profile memory (item 39), as described in column 6 lines 1 to 11. Also, the communication module (item 34) allows intrusion detection device access the data in database handler (item 26). This clearly allows the intrusion detection device access the functionality of the data monitoring device to perform intrusion detection, and hence discloses the feature. (Vaidya does not specifically refer to an application program interface to access the data and functionalities of the data monitoring device. Therefore, the Examiner asserts that Vaidya discloses the feature); and

a computer-readable storage medium for storing codes (Fig. 2 item 39 and associated description).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

FH

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100